The 7th InfoSecurity Summit 2015 – Hong Kong
24th April, 2015 (Friday)
Hong Kong Convention and Exhibition Centre

Making businesses more secure and resilient in a digital world

TENTATIVE CONFERENCE PROGRAM

08:15 – 09:00	**Registration**
08:50 – 09:00	**Opening Remarks:** Officiating VIP Guest: Victor Lam, JP Government Chief Information Officer (Acting) The Government of the HKSAR
09:00 – 09:30	**Opening Keynote: Cyber Risk in a Digital World** Digitization is dramatically changing how organizations work, leading to increasing cyber risk concerns as it opens up the enterprise. Managing these inappropriately can either slow down business innovation or leave critical risks unaddressed. This session will share the core beliefs and key imperatives for handling cyber risk in the digital world, resulting in a resilient cybersecurity operating model and new ways of working for the digital enterprise. Opening Keynote: Harrison Lung Associate Partner McKinsey & Company
09:30 – 10:00	**Keynote 1: Innovative Approach to Protect Against Advanced Persistent Threats (APTs)** As high-profile targeted attacks expand and evolve, enterprises and government departments must guard against complex, often invisible threats. A protection that goes beyond the limitations of standard defenses to detect and analyze attacks in real-time, actively prevents network intrusion and contains threats will help organisations achieve a new level of defense against advanced threats. In this session HP will join Trend Micro to introduce an innovative approach to defeat targeted attacks. Kelvin Wee, Regional Product Manager – APJ, HP Tony Lee, Consultant, Trend Micro
10:00 – 10:30	**Keynote 2: It's When, Not If.** **1 Billion Data Records Stolen in 2014** 66% percent of security breaches remain undiscovered for months or longer. Are you 100% sure that you would know that your organization had been breached, how, when and where? Detecting today's advanced threats requires greater visibility and understanding of network activity. However, the sheer volume of processes, services and applications running on a corporate network at any given time makes it difficult to distinguish abnormal or suspicious network activity. Suspicious activity can go unnoticed for long periods of time, and may only be noticed when it's too late. **Bill Taylor, Vice President of LogRhythm Asia Pacific & Japan** will present an insightful session where he will share how LogRhythm's patented and award-winning Security Intelligence solution gives real-time network visibility that creates actionable Security Intelligence so that organizations can respond quickly to today's highly sophisticated cyber threats and avoid

	material damage. Bill Taylor Senior Vice President & General Manager, Asia Pacific and Japan LogRhytnm
10:30 – 11:00	**Keynote 3: Highway to Hell or Stairway to Heaven? The privileged pathway of targeted attacks** Targeted attacks are the most emphasized growing cyber threat to organizations in recent years, and in the foreseeable future. Organizations that once relied on perimeter defenses understand that when targeted, their perimeter will not withstand the attack. Mitigation focus should shift to inside the network, so as to - prevent the attacker from operating there, - detect any malicious activity - set up response capabilities to minimize damage. The attackers are looking for privileges that will enable them to operate in the network and to get to their goals. In this presentation we will explore the privilege escalation cycle model - which identifies the main steps an attacker takes inside the network - and apply it to recent breaches. We will also look at how anomaly detection learns normal behavior in the network and detects anomalies that may indicate malicious activity. The presentation will show how, by focusing on the privileged activity in the network, protecting the privileged accounts and detecting their abuse, you can mitigate targeted attacks and minimize the damage to your organization. Dan Dinnar Regional Director CyberArk Software, Ltd
11:00 – 11:15	**Morning Networking Coffee Break and Showcase Tour**
11:15 – 11:45	**Keynote 4: Remove the Fear Factor - Risk Assessment in Cloud** In a post-Snowden world, decision makers are facing the challenge to balance the risks and rewards of using cloud solution. While the cost benefits of using cloud is obvious, how do we ensure we only take the benefits without getting the associated risks? This presentation will discuss the following topics/questions: • Fundamental differences between Cloud and On-Premise • How to comply with data privacy regulations? • Latest security standards • Requirements from monetary authorities when using cloud • Mitigating risks from cloud solutions

	Philip Poon Information Security Architect Workday
11:45 – 12:15	**Keynote 5: The Hunted becomes the Hunter - Combating Cyber Attacks Through Advanced Analytics & Intelligence** Targeted attacks and advanced malware continue to create untenable cyber risk for even the best security teams. In this session, the speaker will take a data-driven look at the science behind this problem and talks real world techniques to advance the ball in incident detection and discuss how to go on the offensive and get farther back in the kill chain, leveraging applied intelligence and analytics concepts used in the defense of the world's largest wholly-owned facilities based network. CF Chui, Solutions Architect, Arbor Networks Morpheus Cheung, Technical Consultant, CISSP, e-Cop
12:15 – 13:05	**Panel Discussion One: Changing Security Strategy to Combat Today's Sophisticated Threats** The cybersecurity landscape has seen dramatic changes in recent years with the advent and evolution of new and ever-present threats. As targeted attacks and advanced adversaries continue to evolve and become increasingly sophisticated, it is difficult to keep pace and stay protected. During the panel discussion, the moderator and panelists will share with us some ways to identify and prevent damage from targeted attacks and discuss with us the current cybersecurity trends, and ways to reveal security threats that elude current defenses. **Panel Chair:** Geoff McClelland, Program Director, CIO Connect HK **Executive Panelists:** Yann Chatreau, Head of IT & Risk Management, Asia Pacific, Allen & Overy Steve Ledzian, Systems Engineering Director – South Asia, Hong Kong & Taiwan, FireEye Dominic Polisano, Vice President, Information Security and Business Continuity Hong Kong Exchanges and Clearing Christoph Ganswindt, Executive Director, Information Technology & Sustainability The Hong Kong Jockey Club Simon Hildenbrand, Group Information Security Office, Compliance & Operational Risk Control, UBS
13:05 – 14:05	**Lunch Break**
14:05 – 14:50	**Panel Discussion Two: Encryption and Access Control for Cloud and Big Data Environments** Cloud and Big Data present unique dilemmas — embracing the benefits of these new technologies while maintaining the security of an organization's assets. When an outside party owns, controls and manages their infrastructure and computational resources, how can CISOs be assured that sensitive data remains private and secure? How do they best protect data in mixed-use cloud and Big Data infrastructure sets? Is it possible to still satisfy the full range of reporting, compliance and regulatory

	requirements? During the panel discussion, the moderator and panelists will discuss how to address data security in cloud and Big Data environments. **Panel Chair:** Kenneth Wong, Partner, PwC **Executive Panelists under invitation:** Fuller Yu, Head of Technology Risk, AIA Anna Gamvros, Partner, IT/Communications & Commercial, Baker & McKenzie Epsilon Ip, Enterprise Security Architect, Cathay Pacific Airways
14:50 – 15:20	**Keynote 6: Know Your Enemy** In today's world, the reality is that a determined adversary can always get in. Social engineering. Spear phishing. Malware. These scary-sounding attack techniques can be designed to deface a government website, halt operations, or quietly steal away with an organization's private data. Malicious intruders used to employ brute-force strategies to infiltrate a network. However, with time they've become savvier and far more deceptive (think sneaking in through a window and leaving without a trace, versus kicking down a door). Today, there are different types of attacker – from hacktivisits, to state-sponsored organizations, to cyber criminals. The current proliferation of malware and other threats have created an entire cyber crime economy. This session will explain commonly used attack methods and offer practical guidance for prevention, detection, and containment. Anwar McEntee Regional Manager, North Asia Rapid7
15:20 – 15:50	**Keynote 7: APTs and me (or you)** Targeted attacks have now become an established part of the threat landscape. Such attacks can be highly complex and may make use of very sophisticated techniques to infiltrate an organisation and steal sensitive data. Nevertheless, many attacks start by 'hacking the human', i.e. by tricking employees into disclosing information that can be used to gain access to corporate resources. This presentation will look at APT trends, consider the human aspect of APTs and suggest some ways we can defend against them. David Emm Principal Security Researcher, Global Research & Analysis Kapersky Lab
15:50 – 16:20	**Keynote 8: User-Based Threats: Identifying Activities and Intent** Are you monitoring your fastest growing threat? Identifying who or what is driving a data breach is crucial for successful remediation and recovery at multiple levels. Most companies focus on traditional infrastructure-based security prevention solutions designed to keep unauthorized users out. Unfortunately, today 76 percent of all breaches stem from user-based threats that involve validated account information that has either been stolen or misused. Because most companies have

	little visibility into what happens inside their systems, this type of security breach often goes undetected for months. Without user activity monitoring, companies are missing a critical security vantage point leaving them vulnerable, exposed to undetected breaches for extended periods and uncertain as to who exactly did what and when. Instead, user activity monitoring follows users inside the system and records every action, keystroke and file they access. By alerting companies to suspicious behavior in real-time – and providing forensic evidence on exactly what happened – user activity monitoring is uniquely able to help companies prevent the loss of sensitive corporate and customer information. Amir Yampel Major Account Director Observe IT
16:20 – 16:30	**Afternoon Networking Coffee Break and Showcase Tour**
16:30 – 17:00	**Closing Keynote: Cyber Security Compliance – the Asia Perspective** Peter Bullock Partner Pinsent Masone
17:00	**End of Conference**